UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

Crystal Brewster, individually, and on behalf of herself and all others similarly situated, Plaintiff, v. Northwell Health, Inc. and Perry Johnson & Associates. Defendant.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Crystal Brewster ("Plaintiff"), on behalf of herself and all others similarly situated ("Class Members"), files this Class Action Complaint ("Complaint") against Defendants Northwell Health, Inc. and Perry Johnson & Associates ("Northwell" and "PJ&A" or, collectively, "Defendants"), and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to safeguard and secure the personally identifiable information ("PII") and personal health information ("PHI") of approximately 3.9 million individuals, including Plaintiff.[1] The individuals affected are former and current patients of Northwell, whose PHI/PII was maintained by PJ&A.

2. The data reportedly exposed in the breach includes some of the most sensitive types of data that cybercriminals seek in order to commit fraud and identity theft. According to

[1] Ishita Tripathi, *Northwell Health Data Breach Exposes Over 3 Million Patient's Details*, CYBER EXPRESS (Nov. 10, 2023), https://thecyberexpress.com/northwell-health-data-breach-patient-data-leak/.

Northwell, information disclosed in the breach includes, but is not limited to, names, dates of birth, addresses, medical record numbers, hospital account numbers, admission diagnoses, dates and times of service, and other clinical information.

3. Northwell is a healthcare provider with a network of twenty hospitals and over 800 outpatient facilities in New York.[2]

4. PJ&A is a vendor which offers transcription services to organizations in the medical, legal, and government sectors.

5. On or about May 2, 2023, PJ&A determined that a malicious actor had gained access to its network systems and accessed the PII of Plaintiff and Class members between March 27, 2023, and May 2, 2023 (the "Data Breach"). PJ&A notified Northwell of the Data Breach on July 21, 2023.

6. Armed with the Personal Information accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial information in Class members' names, taking out loans in Class members' names, using Class members' names to obtain medical services, and using Class members' health information to target other phishing and hacking intrusions based on their individual.

7. Defendants owed a non-delegable duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PHI/PII against unauthorized access and disclosure.[3] Defendants breached that

[2] *About Northwell*, NORTHWELL HEALTH, https://www.northwell.edu/about-northwell (last visited Nov. 20, 2023).

[3] Defendants also understood the need to safeguard the PHI/PII it collects and maintains for its financial benefit, as reflected by their privacy policies posted on their websites. *See infra* note 8.

duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its customers' PHI/PII from unauthorized access and disclosure.

8. As a result of Defendants' inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PHI/PII was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons whose PHI/PII was exposed as a result of the Data Breach, which Defendants learned of on or about May 2, 2023, and first publicly acknowledged on November 3, 2023.

9. As a result of the Data Breach, Plaintiff and Class members have been exposed to a heightened and imminent risk of medical and financial fraud and identity theft. Plaintiff and Class members must now and in the future closely monitor their financial accounts and medical information to guard against identity theft.

10. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief, including improvements to Defendants' data security system, future annual audits, and adequate credit monitoring services funded by Defendants.

11. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, and unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

12. Plaintiff Crystal Brewster is a New York resident. On November 3, 2023, Plaintiff Brewster received a letter from Defendants notifying her that her PHI/PII was among the

information accessed by cybercriminals in the Data Breach.[4] Had Plaintiff Brewster known that Defendants would not adequately protect her and Class members' PHI/PII, she would not have received services from Defendants or any of its affiliates and would not have provided her PHI/PII to Defendants or any of its affiliates.

13. Defendant Northwell Health, Inc. is a nonprofit organization with its principal place of business in New Hyde Park, New York.

14. Defendant Perry Johnson & Associates is a corporation with its principal place of business in Henderson, Nevada.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interests and costs.

16. This Court has diversity jurisdiction over Plaintiff's claims pursuant to 29 U.S.C. § 1332(a)(1) because Plaintiff and Defendants are citizens of different states and the amount in controversy exceeds $75,000.

17. This Court has general personal jurisdiction over Defendant Northwell because Northwell maintains its principal place of business in New Hyde Park, New York, regularly conducts business in New York, and has sufficient minimum contacts in New York. Northwell

[4] As reflected in the Incident Notice letter Plaintiff Brewster received on November 3, 2023, Plaintiff Crystal Brewster was previously known as Sequann Brewster. As of March 14, 2021, per a Certified Order of NYC Civil Court, Queens County, she was authorized to assume her current name of Crystal Brewster.

engaged in the conduct underlying this action in New York, including the collection, storage, and inadequate safeguarding of Plaintiff's and Class members' PHI/PII.

18. This Court has general personal jurisdiction over Defendant PJ&A because PJ&A regularly conducts business in New York and has sufficient minimum contacts in New York. PJ&A engaged in the conduct underlying this action in New York, including the collection, storage, and inadequate safeguarding of Plaintiff's and Class members' PHI/PII.

19. Venue in proper in this District pursuant to 28 U.S.C. § 1391(b) because Northwell's principal place of business is in this District, and a substantial part of the events giving rise to this action occurred in this District. Within this District, Defendants entered into consumer transactions with Plaintiff, provided healthcare services, and made its data security decisions leading to the Data Breach.

FACTUAL ALLEGATIONS

Overview of Defendants

20. As "the largest health system in New York," Northwell treats over two million New Yorkers each year," has more than 85,000 employees, including "more than 12,000 credentialed physicians, more than 19,000 nurses, and more than 5,000 volunteers[,]" and more than 900 hospitals and care centers.[5]

21. In the regular course of its business, Northwell collects and maintains the PHI/PII of its patients.

22. Plaintiff and Class members are, or were, patients at Northwell.

[5] *About Northwell*, *supra* note 2.

23. PJ&A serves as a medical vendor to Northwell and its subsidiaries and affiliates to provide transcription and dictation services. In doing so, PJ&A receives PHI/PII regarding Northwell patients.

The Data Breach

24. On or about May 2, 2023, PJ&A discovered that unauthorized users had gained access to its electronic systems.

25. Following an investigation, PJ&A determined that the Data Breach occurred between March 27, 2023 and May 2, 2023, and the unauthorized access to Northwell patient data specifically occurred between April 7, 2023 and April 19, 2023.

26. On July 21, 2023, PJ&A notified Northwell that an unauthorized actor gained access to and downloaded certain files from their systems.

27. Per news reports, PJ&A "confirmed to the HHS Office for Civil Rights that 8,952,212 individuals were affected, making this one of the largest healthcare data breaches ever discovered."[6] Reports also indicate that Northwell "issued a draft statement saying 3,891,565 individuals had been affected, but that statement was later retracted and the final total has not yet been confirmed."[7]

28. To date, Defendants has not disclosed crucial information, including, but not limited to: how many of its patients were affected by the Data Breach; how the cybercriminals

[6] Steve Alder, *New York's Largest Health System Affected by PJ&A Data Breach*, HIPAA J. (Nov. 13, 2023), https://www.hipaajournal.com/northwell-health-pja-data-breach/.

[7] Steve Alder, *PJ&A Data Breach: Almost 9 Million Patients Affected*, HIPAA J. (Nov. 15, 2023), https://www.hipaajournal.com/pja-data-breach/.

were able to exploit vulnerabilities in Defendants' IT security systems; or the identity of the hacking group responsible for the Data Breach.

29. While Defendants have not disclosed the exact data obtained in the data breach, upon information and belief, the data likely consists of PHI/PII including, but not limited to, names, dates of birth, addresses, medical record numbers, hospital account numbers, admission diagnoses, dates and times of service, and other clinical information.

Defendants Knew That Criminals Target PII

30. At all relevant times, Defendants knew, or should have known, Plaintiff's, and all other Class members', PHI/PII was a target for malicious actors.[8] Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PHI/PII from cyber-attacks that Defendants should have anticipated and guarded against.

31. Defendants' data security obligations are and were particularly important given the substantial increase in cyberattacks and/or data breaches widely reported in the last few years. In fact, in the wake of this rise in data breaches, the Federal Trade Commission has issued an abundance of guidance for companies and institutions that maintain individuals' PII.[9]

---

[8] *Privacy policies & disclaimers*, NORTHWELL HEALTH, https://www.northwell.edu/privacy-policies-disclaimers (last visited Nov. 20, 2023) ("We employ commercially reasonable measures to safeguard the collection, transmission, and storage of the information we collect. These measures vary based on the sensitivity of the information that we collect, process and store and the current state of technology."); *HIPAA Compliancy*, PJ&A, https://www.pjats.com/hipaa-compliancy (last visited Nov. 20, 2023) ("PJ&A recognizes the importance of information security. Comprehensive policies and procedures are used to ensure that all access to patient data is restricted.").

[9] *See, e.g.*, *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited Oct. 25, 2023).

32. PHI/PII is a valuable property right.[10] The value of PHI/PII as a commodity is measurable.[11] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[12] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[13] In fact, it is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

33. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

---

[10] See Marc van Lieshout, The Value of Personal Data, 457 IFIP ADVANCES IN INFO. AND COMMC'N TECH. 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . .").

[11] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[12] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[13] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

34. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[14] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[15] A study by Experian found that the "average total cost" of medical identity theft is "about 20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[16]

35. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank account information, complete with account and routing numbers, can fetch up to $,200 to $1,300 each on the black market.[17] According to a report released by the Federal Bureau of Investigation's Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[18]

---

[14] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAG. (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black).

[15] *Id.*

[16] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 A.M.), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.

[17] SC Staff, *Health insurance credentials fetch higher prices in the online black market*, SC MAG. (Jul. 16, 2023), https://www.scmagazine.com/news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[18] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

36. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[19] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[20] A study by Experian found that the "average total cost" of medical identity theft is "about 20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[21]

37. Consumers place a high value on the privacy of their PII. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[22]

38. Given these factors, any company that transacts business with a consumer and then compromises the privacy of consumers' PHI/PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

39. Therefore, Defendants clearly knew or should have known of the risks of data breaches and thus should have ensured that adequate protections were in place.

---

[19] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAG. (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black).

[20] *Id.*

[21] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 A.M.), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.

[22] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

Theft of PHI/PII has Grave and Lasting Consequences for Victims

40. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victim's name, lock the victim out of his or her financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.[23]

41. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[24] In addition, identity thieves may obtain a job using the victim's Social Security Number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[25]

42. Identity theft victims are frequently required to spend many hours and large sums of money repairing the adverse impact to their credit.

43. Indeed, Plaintiff Brewster has already begun the long and arduous process of preventing further harm and injury resulting from the Data Breach, as she has been forced to

---

[23] *See* Laura Pennington, *Recent Data Breach Trends Mean Your Info Was Likely Stolen Last Year*, TOP CLASS ACTIONS (Jan. 28, 2019), https://topclassactions.com/lawsuit-settlements/privacy/data-breach/875438-recent-data-breach/.

[24] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[25] *See Warning Signs of Identity Theft*, FED. TRADE COMM'N, https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last visited Oct. 25, 2023).

undergo the arduous and time-consuming process of requesting a new social security number, and she has been receiving extraordinary amounts of spam calls, resulting in significant lost time.

44. As the United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report"), identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[26] As the GAO Report states, this type of identity theft is more harmful than any other because it often takes time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

45. In addition, the GAO Report states that victims of this type of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[27]

46. There may be a time lag between when PHI/PII is stolen and when it is used.[28] According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm

---

[26] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T ACCOUNTABILITY OFF. (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[27] *Id.* at 2, 9.

[28] For example, on average, it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information. John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), https://www.iiisci.org/Journal/PDV/sci/pdfs/IP069LL19.pdf.

> resulting from data breaches cannot necessarily rule out all future harm.[29]

47. Such personal information is such a crucial commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security Numbers, and other PHI/PII directly on various Internet websites making the information publicly available.

48. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[30]

49. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft, and some need over a year.[31]

50. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records

---

[29] *Id.* at 29 (emphasis added).

[30] Patrick Lucas Austin, *'It is Absurd.' Data Breaches Show It's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 P.M.), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[31] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends and Workplaces*, IDENTITY THEFT RES. CTR., https://www.idthecenter.org/identity-theft-aftermath-study/ (last visited Nov. 4, 2022).

that can plague victims' medical and financial lives for years."[32] It is "also more difficult to detect, taking almost twice as long as normal identity theft."[33] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PHI/PII "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[34] The FTC also warns, "If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[35]

51. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PHI/PII is forever in cyberspace and was taken by people willing to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

52. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PHI/PII; (iii) deprivation of the value of their

---

[32] Pam Dixon and John Emerson, *Report: The Geography of Medical Identity Theft*, WORLD PRIV. F. 6 (Dec. 12 2017), https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/.

[33] *Health Care Systems and Medical Devices at Risk . . ., supra* n. 17.

[34] *What to Know About Medical Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Nov. 20, 2023).

[35] *Id.*

PHI/PII, for which there is a well-established national and international market; (iv) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face; and (v) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

53. This action is brought and may be properly maintained as a class action pursuant to Rule 23(b)(2) and (3) of the Federal Rules of Civil Procedure.

54. Plaintiff brings this action on behalf of herself and all members of the following Class of similarly situated persons:

> All persons whose PII was accessed in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

55. Plaintiff reserves the right to amend the above definition, or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

56. Plaintiff is a member of the Class.

57. Excluded from the Class is Northwell Health, Inc. and its affiliates, parents, subsidiaries, officers, agents, and directors; Perry Johnson & Associates and its affiliates, parents, subsidiaries, officers, agents, and directors; and the judge(s) presiding over this matter and the clerks of said judge(s).

58. This action seeks both injunctive relief and damages.

59. Plaintiff and the Class satisfy the requirements for class certification for the following reasons:

60. **Numerosity of the Class.** The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. While the exact number of

Class members is unknown at this time, Class members are readily identifiable in Defendants' records, which will be a subject of discovery. Upon information and belief, there are millions of Class members in the Class.

61. **Common Questions of Law and Fact.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether Defendants' data security systems prior to the Data Breach met the requirements of relevant laws;
b. Whether Defendants' data security systems prior to the Data Breach met industry standards;
c. Whether Defendants owed a duty to Plaintiff and Class members to safeguard their PHI/PII;
d. Whether Defendants breached its duty to Plaintiff and Class members to safeguard their PHI/PII;
e. Whether Defendants failed to provide timely and adequate notice of the Data Breach to Plaintiff and Class members;
f. Whether Plaintiff's and Class members' PII was compromised in the Data Breach;
g. Whether Plaintiff and Class members are entitled to injunctive relief; and
h. Whether Plaintiff and Class members are entitled to damages as a result of Defendants' conduct.

62. **Typicality.** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiff and Class members all had their PII stolen in the Data Breach. Plaintiff's grievances, like the proposed Class members' grievances, all arise out of the same business practices and course of conduct by Caesar.

63. **Adequacy of Representation.** Plaintiff will fairly and adequately represent the Class on whose behalf this action is prosecuted. Her interests do not conflict with the interests of the Class.

64. Plaintiff and her chosen attorneys -- Finkelstein, Blankinship, Frei-Pearson & Garber, LLP ("FBFG") -- are familiar with the subject matter of the lawsuit and have full knowledge of the allegations contained in this Complaint.

65. FBFG has been appointed as lead counsel in several complex class actions across the country and has secured numerous favorable judgments in favor of its clients, including in cases involving data breaches. FBFG's attorneys are competent in the relevant areas of the law and have sufficient experience to vigorously represent the Class members. Finally, FBFG possesses the financial resources necessary to ensure that the litigation will not be hampered by a lack of financial capacity and is willing to absorb the costs of the litigation.

66. **Predominance.** The common issues identified above arising from Defendants' conduct predominate over any issues affecting only individual Class members. The common issues hinge on Defendants' common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

67. **Superiority.** A class action is superior to any other available method for adjudicating this controversy. The proposed class action is the surest way to fairly and expeditiously compensate such a large a number of injured persons, to keep the courts from becoming paralyzed by hundreds -- if not thousands -- of repetitive cases, and to reduce transaction costs so that the injured Class members can obtain the most compensation possible.

68. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in

the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendants has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendants to all Class members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class members are forced to bring individual suits, the transactional costs, including those incurred by Defendants, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with the identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class members and as to Defendants.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only patients of Northwell Health, Inc., the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class members can be identified from Defendants' records, such that direct notice to the Class members would be appropriate.

69. **Injunctive relief.** Caesars has acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final injunctive or equitable relief on a class-wide basis.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

70. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

71. Defendants owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PHI/PII in its possession, custody, or control.

72. As a condition of receiving Defendants' services, Plaintiff and Class members were required to provide Defendants with their PHI/PII.

73. Defendants knew the risks of collecting and storing Plaintiff's and all other Class members' PHI/PII and the importance of maintaining secure systems. Defendants knew of the many data breaches that targeted companies that store PHI/PII in recent years.

74. Given the nature of Defendants' businesses, the sensitivity and value of the PHI/PII they maintain, and the resources at its disposal, Defendants should have identified the vulnerabilities in their systems and prevented the Data Breach from occurring.

75. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PHI/PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PHI/PII entrusted to them—including Plaintiff's and Class members' PHI/PII.

76. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PHI/PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PHI/PII to unauthorized individuals.

77. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PHI/PII would not have been compromised.

78. As a result of Defendants' above-described wrongful actions, inaction, and lack of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PHI/PII; (iii) breach of the confidentiality of their PHI/PII; (iv) deprivation of the value of their PHI/PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

79. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

80. Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

81. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendants, of failing to employ reasonable measures to protect and secure PHI/PII.

82. Defendants violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PHI/PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PHI/PII is obtains and stores, and the foreseeable consequences of a data breach involving PHI/PII including, specifically, the substantial damages that would result to Plaintiff and other Class members.

83. Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitute negligence per se.

84. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

85. The harm occurring as a result of the Data Breach is the type of harm against which HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard.

86. It was reasonably foreseeable to Defendants that their failure to exercise e reasonable care in safeguarding and protecting Plaintiff's and Class members' PHI/PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PHI/PII to unauthorized individuals.

87. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for

protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PHI/PII; (iii) breach of the confidentiality of their PHI/PII; (iv) deprivation of the value of their PHI/PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

88. Caesars' violations of the FTCA and state data security statutes constitute negligence *per se* for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were designed to protect a group to which Plaintiff belongs and to prevent the type of harm that resulted from the Data Breach.

89. Caesars owed a duty of care to the Plaintiff and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

90. It was foreseeable that Caesars' failure to use reasonable measures to protect PII and to provide timely notice of the Data Breach would result in injury to Plaintiff and other Class members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

91. It was therefore foreseeable that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card

statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
BREACH OF FIDUCIARY DUTY

92. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

93. Plaintiff and Class members gave Defendants their PHI/PII in confidence, believing that Defendants would protect that information. Plaintiff and Class members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance and storage of Plaintiff's and Class members' PHI/PII created a fiduciary relationship between Defendants and Plaintiff and Class members. In light of this relationship, Defendants must act primarily for the benefit of its patients and former patients, which includes safeguarding and protecting Plaintiff's and Class members' PHI/PII.

94. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. They breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class members' PHI/PII and otherwise failing to safeguard Plaintiff's and Class members' PHI/PII that they collected.

95. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer injury, including, but not limited to: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) the improper compromise, publication, and theft of their PHI/PII; (iii) deprivation of the value of their PHI/PII, for which there is a well-established national and international market; (iv) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach,

including the increased risks of identity theft they face and will continue to face; (v) the continued risk to their PHI/PII which remains in Defendants' possession; and (vi) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT

96. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

97. In connection with receiving medical services, Plaintiff and all other Class members entered into implied contracts with Defendants.

98. Pursuant to these implied contracts, in exchange for the consideration and PII provided by Plaintiff and Class members, Defendants agreed to, among other things, and Plaintiff understood that Defendants would: (1) provide medical services to Plaintiff and Class members; (2) implement reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PHI/PII; and (3) protect Plaintiff's and Class members' PHI/PII in compliance with federal and state laws and regulations and industry standards.

99. The protection of PII was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Defendants, on the other hand. Indeed, as set forth *supra*, Defendants recognized its duty to provide adequate data security and ensure the privacy of its consumers' PHI/PII with its practice of providing a privacy policy on its website.[36] Had Plaintiff and Class members known that Defendants would not adequately protect its patients' and former patients' PHI/PII, they would not have received services from Defendants.

[36] *See supra* note 8.

100. Plaintiff and Class members performed their obligations under the implied contract when they provided Defendants with their PHI/PII and paid for the services from Defendants.

101. Defendants breached their obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PHI/PII and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PHI/PII in a manner that complies with applicable laws, regulations, and industry standards.

102. Defendants' breach of their obligations of their implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

103. Plaintiff and all other Class members were suffered by Defendants' breach of implied contracts because: (i) they paid for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; (vi) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT V
UNJUST ENRICHMENT

104. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

105. This claim is pleaded in the alternative to the breach of implied contract claim.

106. Plaintiff and Class members conferred a monetary benefit upon Defendants in the form of monies paid for health care or other services.

107. Defendants accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members. Defendants also benefitted from the receipt of Plaintiff's and Class members' PHI/PII, as this was used to facilitate payment.

108. As a result of Defendants' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

109. Defendants should not be permitted to retain the money belonging to Plaintiff and Class members because Defendants failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

110. Defendants should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in his favor and against Caesars as follows:

A. Certifying that Class as requested herein, appointing the named Plaintiff as Class representative and the undersigned counsel as Class Counsel;

B. Requiring that Defendants pay for notifying the members of the Class of the pendency of this suit;

C. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

D. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend additional credit monitoring services and similar services to protect against all types of identity theft and medical identity theft.

E. Awarding Plaintiff and the Class prejudgment and post-judgment interest to the maximum extent allowable;

F. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable, together with their costs and disbursements of this action; and

G. Awarding Plaintiff and the Class such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: November 20, 2023

Respectfully submitted,

/s/ Todd S. Garber

Todd S. Garber
Andrew C. White
FINKELSTEIN, BLANKINSHIP FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, New York 10601
Tel.: (914) 298-3281

tgarber@fbfglaw.com
awhite@fbfglaw.com